



5-8-01

09CD
#2

501.39942X00

T

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): M. NISHIOKA, ET AL .
Serial No.: 09 / 828,213
Filed: APRIL 9, 2001
Title: "PUBLIC KEY ENCRYPTION METHOD AND COMMUNICATION
SYSTEM USING PUBLIC KEY CRYPTOSYSTEM".

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

MAY 9, 2001

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s)
the right of priority based on:

Japanese Patent Application No. 2000 - 208237
Filed: JULY 5, 2000

A certified copy of said Japanese Patent Application is attached.

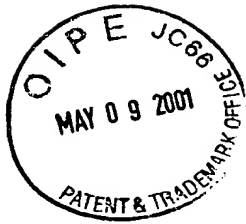
Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundage
Registration No. 29,621

CIB/rp
Attachment

340001039021
501.39942X00



日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 7月 5日

出 願 番 号

Application Number:

特願2000-208237

出 願 人

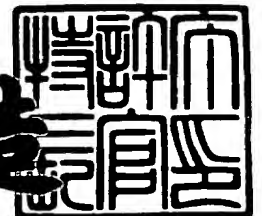
Applicant (s):

株式会社日立製作所

2001年 4月13日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3029961

【書類名】 特許願

【整理番号】 K00010391

【提出日】 平成12年 7月 5日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【請求項の数】 47

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 西岡 玄次

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 佐藤 尚宜

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 梅木 久志

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 瀬戸 洋一

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社日立製作所

【代理人】

 【識別番号】 100075096

 【弁理士】

 【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 公開鍵暗号方法および公開鍵暗号を用いた通信システム

【特許請求の範囲】

【請求項 1】

送信者側装置が、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号を用いた通信方法であって、

鍵生成のステップとして、

【数 1】

- p, q : 素数, $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵 (p, q, β) を作成し、さらに、

【数 2】

- $n = p^d q$ ($d > 1$ は奇数)
- k : pq のビット長
- $\alpha \in \mathbb{Z}$

なる公開鍵 (n, k, α) を作成し、

(1) 送信者側装置は、暗号化ステップとして、平文 $m (0 < m < 2^{k-2})$ に対して、

【数 3】

$$C = m^{2n\alpha} \bmod n$$

を計算し、さらに Jacobi 記号 $a = (m/n)$ を計算し、 (C, a) を暗号文として前記受信者側装置に送信し、

(2) 前記受信者側装置は、復号化ステップとして、受信者の秘密鍵 (p, q, β) を用いて、暗号文 (C, a) から、

【数 4】

$$\begin{aligned} m_{1,p} &= C^{\frac{(p+1)\beta q^{-1}}{4}} \bmod p, \\ m_{1,q} &= C^{\frac{(q+1)\beta p^{-d}}{4}} \bmod q \end{aligned}$$

を計算し、 $\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$,

$\phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たすものを平文 m とする(但し、 ϕ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。),

公開鍵暗号を用いた通信方法。

【請求項 2】

請求項1において、前記公開情報 (n, k, α) は、前記受信者側装置が生成し、公開するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 3】

請求項1または請求項2において、 $\alpha = \beta = 1$ の場合については、 α 、 β の各々を公開鍵、秘密鍵から削除する

公開鍵暗号を用いた通信方法。

【請求項 4】

送信者側装置は、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号を用いた通信システムであって、

【数 5】

- p, q : 素数, $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵 (p, q, β) と、

【数 6】

- $n = p^d q$ ($d > 1$ は奇数)
- k : pq のビット長
- $\alpha \in \mathbb{Z}$
- $a \in \{-1, 1\}$

なる公開鍵 (n, k, α, a) (但し、 k は pq のビット長)とを作成する鍵生成装置と、

(1) $a = (m/n)$ なる平文 $m(0 < m < 2^{k-2})$ に対して(但し、 $a = (m/n)$ はJacobi記号を表す),

【数 7】

$$C = m^{2n\alpha} \bmod n$$

を計算する装置と、

Cを暗号文として受信者側装置に送信する通信装置と
を備える送信者側装置と、

(2)受信者の秘密鍵 (p, q, β) を用いて、暗号文Cから、

【数 8】

$$\begin{aligned} m_{1,p} &= C^{\frac{(p+1)\beta q^{-1}}{4}} \bmod p, \\ m_{1,q} &= C^{\frac{(q+1)\beta p^{-1}}{4}} \bmod q \end{aligned}$$

を計算する装置と、

$\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n) = a$ かつ $0 < x < 2^{k-2}$ を満たすものを平文 m (但し、 ϕ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。)を求める装置とを備える受信者側装置と

からなる、公開鍵暗号を用いた通信システム。

【請求項 5】

請求項4において、

前記受信者側装置は、前記公開情報 (n, k, α, a) を生成する装置を備える公開鍵暗号を用いた通信システム。

【請求項 6】

請求項4または請求項5において、 $\alpha = \beta = 1$ の場合については、 α, β の各々を公開鍵、秘密鍵から削除する装置を備える公開鍵暗号を用いた通信システム。

【請求項 7】

請求項1ないし請求項3のいずれかにおいて、

秘密鍵 p, q は、素数 p', q' から $p=2p'+1, q=2q'+1$ により作成するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 8】

請求項1ないし請求項3または請求項7のいずれかにおいて、

送信者が受信者に対し送信したいメッセージ文に対して、正しく復号されたか

を確認するための検査情報を含むように平文 m を作成するステップを備える
公開鍵暗号を用いた通信方法。

【請求項 9】

請求項1ないし請求項3または請求項7または請求項8のいずれかにおいて、
送信者が受信者に対し送信したいメッセージ文に対して、予め定められた冗長性を持たせた内容を平文 m とし、該請求項1または請求項4に記載の方法により暗号化するステップを備え、

受信者側装置は、該請求項1または請求項4に記載の方法により平文 m を復号化し、予め定められた冗長性を確認するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 10】

請求項1ないし請求項3または請求項7または請求項8のいずれかにおいて、
送信者が受信者に対し送信したいメッセージ文に対して、予め定められた意味のあるメッセージを加えた内容を平文 m とし、該請求項1または請求項4に記載の方法により暗号化するステップを備え、

受信者側装置は、該請求項1または請求項4に記載の方法により平文 m を復号化し、予め定められた意味のあるメッセージの内容を確認するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 11】

請求項1ないし請求項3または請求項7ないし請求項10のいずれかにおいて、

$d (d > 1)$ の値を可変とする

公開鍵暗号を用いた通信方法。

【請求項 12】

送信者側装置は、受信者の公開鍵を用いて暗号通信を行なうための鍵共有方法であって、

鍵生成のステップとして、

【数 9】

- p, q : 素数, $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵 (p, q, β) を作成し、さらに、

【数 1 0】

- $n = p^d q$ ($d > 1$ は奇数)
- k : pq のビット長
- $\alpha \in \mathbb{Z}$
- f : 一方向性関数

なる公開鍵 (n, k, α) を作成し(但し、 k は pq のビット長)、

(1)送信者側装置は、共有鍵 $K=f(m)$ を受信者側装置と共有することを目的として、送信データ $m(0 < m < 2^{k-2})$ に対して、

【数 1 1】

$$C = m^{2n\alpha} \bmod n$$

を計算し、さらにJacobi記号 $a=(m/n)$ 、及び、共有鍵 K を $K=f(m)$ にて計算し、 (C, a) を暗号文として前記受信者側装置に送信し、

また、送信者側装置は、共有鍵 $K=f(m)$ を計算し、

(2)前記受信者側装置は、受信者の秘密鍵 (p, q, β) を用いて、暗号文 (C, a) から、

【数 1 2】

$$\begin{aligned} m_{1,p} &= C^{\frac{(p+1)2q^{-1}}{4}} \bmod p, \\ m_{1,q} &= C^{\frac{(q+1)2p^{-1}}{4}} \bmod q \end{aligned}$$

を計算し、 $\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たすものを送信データ m として計算し(但し、 ϕ は中国人の剰余定理による $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ から $\mathbb{Z}/(pq)$ への環同型写像を表す。), さらに、公開情報 f を用いて共有鍵 K を $K=f(m)$ により計算する鍵共有方法。

【請求項 1 3】

請求項12において、前記公開情報 (n, k, α) は、前記受信者側装置が生成し、公開するステップを備える

鍵共有方法。

【請求項 1 4】

請求項12または請求項13において、 $\alpha = \beta = 1$ の場合については、 α 、 β の各々を公開鍵，秘密鍵から削除する鍵共有方法。

【請求項 1 5】

送信者側装置は、受信者の公開鍵を用いて暗号通信を行なうための鍵共有方法であって、

鍵生成のステップとして、

【数 1 3】

- p, q : 素数、 $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵 (p, q, β) を作成し、さらに、

【数 1 4】

- $n = p^d q$ ($d > 1$ は奇数)
- k : pq のビット長
- $\alpha \in \mathbb{Z}$
- $a \in \{-1, 1\}$
- f : 一方向性関数

なる公開鍵 (n, k, α, a) を作成し(但し、 k は pq のビット長)、

(1)送信者側装置は、共有鍵 $K=f(m)$ を受信者側装置と共有することを目的として、 $a=(m/n)$ なる送信データ $m(0 < m < 2^{k-2})$ に対して(但し、 $a=(m/n)$ はJacobi記号を表す)、

【数 1 5】

$$C = m^{2n\alpha} \bmod n$$

を計算し、さらに共有鍵 K を $K=f(m)$ にて計算し、 C を暗号文として前記受信者側装置に送信し、

また、送信者側装置は、共有鍵 $K=f(m)$ を計算し、

(2)前記受信者側装置は、受信者の秘密鍵 (p, q, β) を用いて、暗号文 C から、

【数 1 6】

$$m_{1,p} = C^{\frac{(p+1)3q-1}{4}} \bmod p,$$

$$m_{1,q} = C^{\frac{(q+1)3p-d}{4}} \bmod q$$

を計算し、 $\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$,
 $\phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たすものを送信データ m とし
 て計算し(但し、 ϕ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同
 型写像を表す。), さらに、公開情報 f を用いて共有鍵 K を $K=f(m)$ により計算する
 鍵共有方法。

【請求項 1 6】

請求項15において、前記公開情報 (n, k, α, a) は、前記受信者側装置が生成し、
 公開するステップを備える

鍵共有方法。

【請求項 1 7】

請求項15または請求項16において、 $\alpha = \beta = 1$ の場合については、 α , β の各
 々を公開鍵、秘密鍵から削除する

鍵共有方法。

【請求項 1 8】

請求項12ないし請求項17のいずれかにおいて、

秘密鍵 p, q は、素数 p', q' から $p=2p'+1$, $q=2q'+1$ により作成するステップを
 備える

鍵共有方法。

【請求項 1 9】

請求項12ないし請求項18のいずれかにおいて、

$d (d > 1)$ の値を可変とする

鍵共有方法。

【請求項 2 0】

請求項1または請求項4において、

単数または複数のハッシュ関数が公開されており、送信者側装置は、平文およ

び乱数情報を作成するステップを備え、

また、該平文および該乱数情報に対して、排他的論理和およびデータの接続による演算を行うステップを備え、

また、該演算により得られた結果を該ハッシュ関数に入力し、その結果を計算するステップを備え、

また、該平文および該乱数情報と該ランダム関数への入力結果に対して排他的論理和およびデータの接続による演算を行うステップを備え、

また、該演算を行った結果を、請求項1または請求項4における平文 m の箇所、または、乱数 r の箇所に置き換え、請求項1または請求項4における公開鍵暗号化方法の手順により暗号化する

公開鍵暗号における暗号化方法。

【請求項 2 1】

請求項20に記載の方法により暗号化した暗号文を復号化する方法において、

請求項1または請求項4に記載の復号化ステップを備え、

請求項20において行われた排他的論理和およびデータの接続による演算結果から平文 m を戻すステップを備え、また、該(排他的論理和およびデータの接続による)演算の手順の正当性を確かめるステップを備え、

復号化結果を出力するステップを備える

公開鍵暗号における復号化方法。

【請求項 2 2】

送信者側装置は、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号を用いた通信方法であって、

鍵生成のステップとして、

【数 1 7】

- p, q : 素数, $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵 (p, q, β) を作成し、さらに、

【数 1 8】

- $n = p^d q$ ($d > 1$ は奇数)
- k, k_0, k_1 : k は pq のビット長, k_0, k_1 は $k > k_0 - k_1 - 2$ なる正整数
- $\alpha \in \mathbb{Z}$
- $G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k-k_0-2}$
- $H : \{0, 1\}^{k-k_0-2} \rightarrow \{0, 1\}^{k_0}$

なる公開鍵 $(n, k, k_0, k_1, \alpha, G, H)$ を作成し,

(1) 送信者側装置は, 平文 $m (m \in \{0, 1\}^l, l = k - k_0 - k_1 - 2)$, および, 乱数 $r (r \in \{0, 1\}^{k_0})$ に対して,

【数 1 9】

$$x = (m0^{k_1} \oplus G(r)) \parallel (r \oplus H(m0^{k_1} \oplus G(r)))$$

を計算し, さらに,

【数 2 0】

$$C = x^{2\pi\alpha} \bmod n$$

を計算し, さらに Jacobi 記号 $a = (x/n)$ を計算し, (C, a) を暗号文として前記受信者側装置に送信し,

(2) 前記受信者側装置は, 受信者の秘密鍵 (p, q, β) を用いて, 暗号文 (C, a) から,

【数 2 1】

$$\begin{aligned} x_{1,p} &= C^{\frac{(p+1)3q^{-1}}{4}} \bmod p, \\ x_{1,q} &= C^{\frac{(q+1)3p^{-1}}{4}} \bmod q \end{aligned}$$

を計算し, $\phi(x_{1,p}, x_{1,q}), \phi(-x_{1,p}, x_{1,q}), \phi(x_{1,p}, -x_{1,q}), \phi(-x_{1,p}, -x_{1,q})$ のうち, $(y/n) = a$ かつ $0 < y < 2^{k-2}$ を満たす y を計算し (但し, ϕ は中国人の剰余定理による

$\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ から $\mathbb{Z}/(pq)$ への環同型写像を表す。),

さらに,

【数 2 2】

$$y = s || t \quad (s \in \{0, 1\}^{k-k_0-2}, t \in \{0, 1\}^{k_0})$$

とするとき,

【数 2 3】

$$z = G(H(s) \oplus t) \oplus s,$$

を計算し,

【数 2 4】

$$m = \begin{cases} [z]^l & \text{if } [z]_{k_1} = 0^{k_1} \\ \text{"reject"} & \text{otherwise} \end{cases}$$

により, 平文 m の復号化を行う(但し, $[a]_k$, $[a]_k$ は各々 a の上位および下位 k ビットを表す。),

公開鍵暗号を用いた通信方法。

【請求項 2 3】

請求項22において, 前記公開情報 $(n, k, k_0, k_1, \alpha, G, H)$ は, 前記受信者側装置が生成し, 公開するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 2 4】

請求項22または請求項23において, $\alpha = \beta = 1$ の場合については, α , β の各々を公開鍵, 秘密鍵から削除する

公開鍵暗号を用いた通信方法。

【請求項 2 5】

送信者側装置は, 受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号を用いた通信方法であって,

鍵生成のステップとして,

【数 2 5】

- p, q : 素数, $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵 (p, q, β) を作成し, さらに,

【数 2 6】

- $n = p^d q$ ($d > 1$ は奇数)
- $k, k_0, k_1 \in \mathbb{Z}$: k は pq のビット長, k_0, k_1 は $k > k_0 - k_1 - 2$ なる正整数
- $\alpha \in \mathbb{Z}$
- $a \in \{-1, 1\}$
- $G: \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k-k_0-2}$
- $H: \{0, 1\}^{k-k_0-2} \rightarrow \{0, 1\}^{k_0}$

なる公開鍵 $(n, k, k_0, k_1, \alpha, a, G, H)$ を作成し,

(1) 送信者側装置は, 平文 $m (m \in \{0, 1\}^l, l = k - k_0 - k_1 - 2)$, および, 乱数 $r (r \in \{0, 1\}^{k_0})$ に対して, $a = (x/n)$ となるような (但し, $a = (m/n)$ は Jacobi 記号を表す)

【数 2 7】

$$x = (m0^{k_1} \oplus G(r)) \parallel (r \oplus H(m0^{k_1} \oplus G(r)))$$

を計算し, さらに,

【数 2 8】

$$C = x^{2n\alpha} \pmod{n}$$

を計算し, C を暗号文として前記受信者側装置に送信し,

(2) 前記受信者側装置は, 受信者の秘密鍵 (p, q, β) を用いて, 暗号文 C から,

【数 2 9】

$$\begin{aligned} x_{1,p} &= C^{\frac{(p+1)\beta q^{-1}}{4}} \pmod{p}, \\ x_{1,q} &= C^{\frac{(q+1)\beta p^{-1}}{4}} \pmod{q} \end{aligned}$$

を計算し, $\phi(x_{1,p}, x_{1,q}), \phi(-x_{1,p}, x_{1,q}), \phi(x_{1,p}, -x_{1,q}), \phi(-x_{1,p}, -x_{1,q})$ のうち, $(y/n) = a$ かつ $0 < y < 2^{k-2}$ を満たす y を計算し (但し, ϕ は中国人の剰余定理による

$Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。),

さらに,

【数 3 0】

$$y = s || t \quad (s \in \{0, 1\}^{k-k_0-2}, t \in \{0, 1\}^{k_0})$$

とするとき,

【数 3 1】

$$z = G(H(s) \oplus t) \oplus s,$$

を計算し,

【数 3 2】

$$m = \begin{cases} [z]^l & \text{if } [z]_{k_1} = 0^{k_1} \\ \text{"reject"} & \text{otherwise} \end{cases}$$

により, 平文 m の復号化を行う (但し, $[a]^k, [a]_k$ は各々 a の上位および下位 k ビットを表す。),

公開鍵暗号を用いた通信方法。

【請求項 2 6】

請求項 25 において, 前記公開情報 $(n, k, k_0, k_1, \alpha, a, G, H)$ は, 前記受信者側装置が生成し, 公開するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 2 7】

送信者側装置は, 受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号を用いた通信方法であって,

鍵生成のステップとして,

【数 3 3】

- p, q : 素数, $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵 (p, q, β) を作成し, さらに,

【数 3 4】

- $n = p^d q$ ($d > 1$ は奇数)
- $k, k_0, k_1 \in \mathbb{Z}$: k は pq のビット長, k_0, k_1 は $k > k_0 - k_1 - 2$ なる正整数
- $\alpha \in \mathbb{Z}$
- $G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k-k_0-2}$
- $H : \{0, 1\}^{k-k_0-2} \rightarrow \{0, 1\}^{k_0}$

なる公開鍵 $(n, k, k_0, k_1, \alpha, G, H)$ を作成し,

(1) 送信者側装置は, 平文 $m (m \in \{0, 1\}^l, l = k - k_0 - k_1 - 2)$, および, 乱数 $r (r \in \{0, 1\}^{k_0})$ に対して,

【数 3 5】

$$x = (m0^{k_1} \oplus G(r)) || (r \oplus H(m0^{k_1} \oplus G(r)))$$

を計算し, さらに,

【数 3 6】

$$C = x^{2n\alpha} \bmod n$$

を計算し, C を暗号文として前記受信者側装置に送信し,

(2) 前記受信者側装置は, 受信者の秘密鍵 (p, q, β) を用いて, 暗号文 C から,

【数 3 7】

$$\begin{aligned} x_{1,p} &= C^{\frac{(p+1)3q-1}{4}} \bmod p, \\ x_{1,q} &= C^{\frac{(q+1)3p-1}{4}} \bmod q \end{aligned}$$

を計算し, 各 $y_1 = \phi(x_{1,p}, x_{1,q}), y_2 = \phi(-x_{1,p}, x_{1,q}),$
 $y_3 = \phi(x_{1,p}, -x_{1,q}), y_4 = \phi(-x_{1,p}, -x_{1,q})$ に対して (但し, ϕ は中国人の剰余定理
 による $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ から $\mathbb{Z}/(pq)$ への環同型写像を表す。),

【数 3 8】

$$y_i = s_i || t_i \quad (s_i \in \{0, 1\}^{k-k_0-2}, t_i \in \{0, 1\}^{k_0}, 1 \leq i \leq 4)$$

とするとき,

【数 3 9】

$$z_i = G(H(s_i) \oplus t_i) \oplus s_i \quad (1 \leq i \leq 4),$$

を計算し,

【数 4 0】

$$m = \begin{cases} [z_i]^l & \text{if } [z_i]_{k_1} = 0^{k_1} \\ \text{"reject"} & \text{otherwise} \end{cases}$$

により, 平文 m の復号化を行う(但し, $[a]^k, [a]_k$ は各々 a の上位および下位 k ビットを表す。),

公開鍵暗号を用いた通信方法。

【請求項 2 8】

請求項27において, 前記公開情報 $(n, k, k_0, k_1, \alpha, G, H)$ は, 前記受信者側装置が生成し, 公開するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 2 9】

請求項22ないし請求項28のいずれかにおいて,

$\alpha = \beta = 1$ の場合については, α, β の各々を公開鍵, 秘密鍵から削除する
公開鍵暗号を用いた通信方法。

【請求項 3 0】

請求項22ないし請求項29のいずれかにおいて,

秘密鍵 p, q は, 素数 p', q' から $p=2p'+1, q=2q'+1$ により作成するステップを
備える

公開鍵暗号を用いた通信方法。

【請求項 3 1】

請求項22ないし請求項30のいずれかにおいて,

$d (d > 1)$ の値を可変とする

公開鍵暗号を用いた通信方法。

【請求項 3 2】

請求項1ないし請求項19のいずれかにおいて、
2つの異なる装置において、暗号文Cを計算する方法であって、
装置1は、平文 $m(0 < m < 2^{k-2})$ に対して、

【数 4 1】

$$C_1 = m^{2\alpha} \bmod n$$

を計算した後、 C_1 を装置2に出力し、装置2は、

【数 4 2】

$$C = C_1^n \bmod n$$

を計算することにより、暗号文Cを計算する
暗号化方法。

【請求項 3 3】

請求項22ないし請求項31のいずれかにおいて、
2つの異なる装置において、暗号文Cを計算する方法であって、
装置1は、平文 $m(m \in \{0,1\}^l, l = k - k_0 - k_1 - 2)$ 、および、乱数 $r(r \in \{0,1\}^{k_0})$ に対して、

【数 4 3】

$$x = (m0^{k_1} \oplus G(r)) \parallel (r \oplus H(m0^{k_1} \oplus G(r)))$$

を計算し、さらに、

【数 4 4】

$$C_1 = x^{2\alpha} \bmod n$$

を計算した後、 C_1 を装置2に出力し、装置2は、

【数 4 5】

$$C = C_1^n \bmod n$$

を計算することにより、暗号文Cを計算する

暗号化方法。

【請求項34】

送信者側装置は、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号を用いた通信方法であって、

鍵生成のステップとして、

【数46】

- p_i : 素数 ($p_i \equiv 3 \pmod{4}$, $1 \leq i \leq h$)
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵 (p_i, β) ($1 \leq i \leq h$) を作成し、さらに、

【数47】

- $n = \prod_{i=1}^h p_i$
- $k, k_0, k_1 \in \mathbb{Z}$: k は n のビット長, k_0, k_1 は $k > k_0 + k_1 - 2$ なる正整数
- $\alpha \in \mathbb{Z}$
- $G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k-k_0}$
- $H : \{0, 1\}^{k-k_0} \rightarrow \{0, 1\}^{k_0}$

なる公開鍵 $(n, k, k_0, k_1, \alpha, G, H)$ を作成し、

(1) 送信者側装置は、平文 m ($m \in \{0, 1\}^l$, $l = k - k_0 - k_1$), および、乱数 r ($r \in \{0, 1\}^k$) に対して、

【数48】

$$x = (m0^{k_1} \oplus G(r)) \parallel (r \oplus H(m0^{k_1} \oplus G(r)))$$

を計算し、さらに、

【数49】

$$C = x^{2\alpha} \bmod n$$

を計算し、C を暗号文として前記受信者側装置に送信し、

(2) 前記受信者側装置は、受信者の秘密鍵 (p_i, β) ($1 \leq i \leq h$) を用いて、暗号文 C から、

【数 5 0】

$$x_i = C^{\frac{(p_i+1)s}{4}} \bmod p_i$$

を計算し、 2^h 個の

$\{\phi(e_1x_1, e_2x_2, \dots, e_hx_h) \mid e_1, \dots, e_h \in \{-1, 1\}\}$ について、

【数 5 1】

$$y_i = s_i || t_i \quad (s_i \in \{0, 1\}^{k-k_0}, t_i \in \{0, 1\}^{k_0}, 1 \leq i \leq 2^h)$$

とするとき、

【数 5 2】

$$z_i = G(H(s_i) \oplus t_i) \oplus s_i \quad (1 \leq i \leq 2^h)$$

を計算し、

【数 5 3】

$$m = \begin{cases} [z_i]^t & \text{if } [z_i]_{k_1} = 0^{k_1} \\ \text{"reject"} & \text{otherwise} \end{cases}$$

により、平文 m の復号化を行う(但し、 ϕ は中国人の剰余定理による $Z/(p_1) \times Z/(p_2) \times \dots \times Z/(p_h)$ から $Z/(n)$ への環同型写像を表す。また、 $[a]^k, [a]_k$ は各々 a の上位および下位 k ビットを表す。),

公開鍵暗号を用いた通信方法。

【請求項 3 5】

請求項34において、前記公開情報 $(n, k, k_0, k_1, \alpha, G, H)$ は、前記受信者側装置が生成し、公開するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 3 6】

請求項34ないし請求項35のいずれかにおいて、

$\alpha = \beta = 1$ の場合については、 α, β の各々を公開鍵、秘密鍵から削除するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 3 7】

請求項34ないし請求項36のいずれかにおいて、

平文 m または x の識別情報を暗号文と共に送信する、または、公開された識別情報から、平文 m または x を作成するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 3 8】

請求項37において、暗号文と共に送信された識別情報、または、公開化された識別情報を利用して、暗号文から該平文 m または該 x を復号化するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 3 9】

請求項1ないし請求項21のいずれかにおいて、

暗号文 C を、

【数 5 4】

$$C = m^{2\alpha} \bmod n$$

にて作成し、 $m_{1,p}$ および $m_{1,q}$ は、

【数 5 5】

$$\begin{aligned} m_{1,p} &= C^{\frac{(p+1)s}{4}} \bmod p, \\ m_{1,q} &= C^{\frac{(q+1)s}{4}} \bmod q \end{aligned}$$

にて作成するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 4 0】

請求項22ないし請求項31のいずれかにおいて、

暗号文 C を、

【数 5 6】

$$C = x^{2\alpha} \bmod n$$

にて作成し、 $m_{1,p}$ および $m_{1,q}$ は、

【数 5 7】

$$m_{1,p} = C^{\frac{(p+1)s}{4}} \bmod p,$$

$$m_{1,q} = C^{\frac{(q+1)s}{4}} \bmod q$$

にて作成するステップを備える

公開鍵暗号を用いた通信方法。

【請求項 4 1】

請求項1ないし3いずれかに記載の、

鍵生成ステップと、暗号化ステップと、復号化ステップのいずれかを計算機に実行させるプログラムと、

当該プログラムを具現化する媒体とからなるプログラム製品。

【請求項 4 2】

送信者側装置と受信者側装置とからなり、前記送信者側装置が、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号を用いた通信システムであって、

前記受信者側装置は、当該受信者側装置が備える演算装置を用いて、

請求項 1 記載の鍵生成のステップを実行し、前記秘密鍵 (p, q, β) と前記公開鍵 (n, k, α) を作成し、

前記送信者側装置は、当該送信者側装置が備える演算装置を用いて、

平文 $m (0 < m < 2^{k-2})$ に対して、請求項 1 記載の暗号化ステップを実行し、

Jacobi 記号 $a = (m/n)$ を計算し、 (C, a) を暗号文として前記受信者側装置に送信し

前記受信者側装置は、当該受信者側装置が備える演算装置を用いて、

請求項 1 記載の復号化ステップを実行し平文 m を求める

公開鍵暗号を用いた通信システム。

【請求項 4 3】

請求項4ないし請求項6のいずれかにおいて、

前記受信者側装置は、秘密鍵 p, q は、素数 p', q' から $p=2p'+1$, $q=2q'+1$ により作成する装置を備える

公開鍵暗号を用いた通信システム。

【請求項 4 4】

請求項4ないし請求項6または請求項43のいずれかにおいて、

送信者側装置は、受信者に対し送信したいメッセージ文に対して、正しく復号されたかを確認するための検査情報を含むように平文 m を作成する装置を備える
公開鍵暗号を用いた通信システム。

【請求項 4 5】

請求項4ないし請求項6または請求項43または請求項44のいずれかにおいて、

前記送信者側装置の平文 m を暗号化する装置は、受信者に対し送信したいメッセージ文に対して、予め定められた冗長性を持たせた内容を平文 m とし、

前記受信者側装置の平文 m を復号化する装置は、予め定められた冗長性を確認する公開鍵暗号を用いた通信システム。

【請求項 4 6】

請求項4ないし請求項6または請求項43または請求項44のいずれかにおいて、

送信者が受信者に対し送信したいメッセージ文に対して、予め定められた意味のあるメッセージを加えた内容を平文 m とし、該請求項1または請求項4に記載の方法により暗号化するステップを備え、

受信者側装置は、該請求項1または請求項4に記載の方法により平文 m を復号化し、予め定められた意味のあるメッセージの内容を確認するステップを備える
公開鍵暗号を用いた通信システム。

【請求項 4 7】

請求項4ないし請求項6または請求項43ないし請求項46のいずれかにおいて、

d ($d > 1$) の値を可変とする公開鍵暗号を用いた通信システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、公開鍵暗号を用いた暗号通信方法および鍵共有方法に関する。

【 0 0 0 2 】

【従来の技術】

現在まで、様々な公開鍵暗号方式が提案されている。なかでも、文献1「R.L.Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, Vol.21, No.2, pp.120-126, 1978.」に掲載されている方法が最も有名であり、最も実用化されている公開鍵暗号である。その他には、文献2「V.S.Miller: Use of Elliptic Curves in Cryptography, Proc. of Crypto'85, LNCS218, Springer-Verlag, pp.417-426 (1985)」, 文献3「N.Koblitz: Elliptic Curve Cryptosystems, Math. Comp., 48, 177, pp.203-209 (1987)」等に記載の楕円曲線を用いた方法が効率的な公開鍵暗号として知られている。

【 0 0 0 3 】

安全性について証明可能な方法として、まず、選択平文攻撃を対象としたものは、文献4「M.O.Rabin: Digital Signatures and Public-Key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCS/TR-212 (1979)」に記載されている暗号方法、文献5「T.ElGamal: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. On Information Theory, IT-31, 4, pp.469-472(1985)」に記載されている暗号方法、文献6「S.Goldwasser and S.Micali: Probabilistic Encryption, JCSS, 28, 2, pp.270-299 (1984)」に記載されている暗号方法、文献7「M.Blum and S.Goldwasser: An Efficient probabilistic public-key encryption scheme which hides all partial information, Proc. of Crypto'84, LNCS196, Springer-Verlag, pp.289-299 (1985)」に記載されている暗号方法、文献8「S.Goldwasser and M.Bellare: Lecture Notes on Cryptography, <http://www-cse.ucsd.edu/users/mihir/> (1997)」に記載されている暗号方法、文献9「T.Okamoto and S.Uchiyama: A New Public-Key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt'98, LNCS1403, Springer Verlag, pp.308-318 (1998)」に記載されている暗号方法、などが知られている。また、選択暗号文攻撃に対して安全性証明可能な方法としては、文献10「D.Dolev, C.Dwork and M.Naor.: Non-malleable cryptography

y, In 23rd Annual ACM Symposium on Theory of Computing, pp.542-552 (1991)」に記載されている暗号方法, 文献11「M.Naor and M.Yung.:Public-key cryptosystems provably secure against chosen ciphertext attacks, Proc. of STOC, ACM Press, pp.427-437 (1990)」に記載されている暗号方法, 文献12「M.Bellare and P.Rogaway,.Optimal Asymmetric Encryption How to Encrypt with RSA, Proc. of Eurocrypt'94, LNCS950, Springer Verlag, pp.92-111 (1994)」に記載されている暗号方法, 文献13「R.Cramer and V.Shoup: A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack, Proc. of Crypto98, LNCS1462, Springer-Verlag, pp.13-25 (1998)」に記載されている暗号方法, などが知られている。

【 0 0 0 4 】

また, 文献14「M.Bellare, A.Desai, D.Pointcheval and P.Rogaway. : Relations Among Notions of Security for Public-Key Encryption Schemes, Proc. of Crypto'98, LNCS1462, Springer Verlag, pp.26-45 (1998)」では, IND-CCA2 (適応的選択暗号文攻撃に対して強秘匿であること)とNM-CCA2(適応的選択暗号文攻撃に対して頑強であること)の等価性が示され, 現在, この条件を満たす公開鍵暗号が最も安全であると考えられている。

【 0 0 0 5 】

【発明が解決しようとする課題】

本発明の主たる目的は, 安全性の証明が可能であり, かつ, 暗復号化処理の効率性に優れる公開鍵暗号方法を提供することにある。

【 0 0 0 6 】

本発明では, 最初に, 素因数分解問題の計算量的複雑さを前提としてOW-CPA(選択平文攻撃に対して一方向)であることが証明可能な公開鍵暗号方法を提供する。さらに, この方法をベースに, IND-CCA2(またはNM-CCA2)であることが証明可能な公開鍵暗号方法を提供する。

【 0 0 0 7 】

これらの暗号方法は, 従来方法に比べて, 暗復号化処理の際に必要なモジュラー積の個数が少なく, 高速な処理が可能となる。

【 0 0 0 8 】

また、本発明の他の目的は、送信データを暗号化する際の計算および暗号化データを復号化する際の計算の負荷が小さく、携帯型情報処理機器など計算能力が限られた装置であっても高速処理が可能な、公開鍵を用いた暗号化方法と復号化方法と、それを用いた鍵配送方法や鍵共有方法、さらには、これらの方法を実行するプログラム、装置またはシステムを提供することである。

【 0 0 0 9 】

【課題を解決するための手段】

上記目的を達成するため、本発明は例えば以下の手段を備える。

(1) $n = p^d q$ (d は $d > 1$ なる奇数)として、 pq のビット長 k に対して平文空間を開区間 $(0, 2^{k-2})$ となるように小さく選ぶ。

【 0 0 1 0 】

(2) 合成数 n (相異なる複数の素数の積からなる数)を法とする剰余群上では、平方根は4個以上存在し、これらの解をうまく利用すると n の素因数分解を行うことができる。このことを利用して、本発明の公開鍵暗号方法では、 n の素因数分解問題の困難性を前提として、選択平文攻撃に対して一方向性(OW-CPA)であることが証明可能となるように暗号化および復号化のための手順を構築する。

【 0 0 1 1 】

(1) 上記(1)、(2)の手段により構成された公開鍵暗号方法に対して、文献12で示されている変換方法を実行し、(理想的)ランダム関数が公開されていることを前提により強固な安全性を持つ方式に変換する。

【 0 0 1 2 】

具体的な方法の1つとしては、

【鍵生成】

【 0 0 1 3 】

【数 5 8】

- p, q : 素数, $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【 0 0 1 4 】

なる秘密鍵 (p, q, β) を作成し、さらに、

【 0 0 1 5 】

【数 5 9】

- $n = p^d q$ ($d > 1$ は奇数)
- k, k_0, k_1 : k は pq のビット長, k_0, k_1 は $k > k_0 - k_1 - 2$ なる正整数
- $\alpha \in \mathbb{Z}$
- $G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k - k_0 - 2}$
- $H : \{0, 1\}^{k - k_0 - 2} \rightarrow \{0, 1\}^{k_0}$

【 0 0 1 6 】

なる公開鍵 $(n, k, k_0, k_1, \alpha, G, H)$ を作成する。

【 0 0 1 7 】

【暗号化】

送信者側装置は、平文 $m (m \in \{0, 1\}^l, l = k - k_0 - k_1 - 2)$ 、および、乱数 $r (r \in \{0, 1\}^{k_0})$ に対して、

【 0 0 1 8 】

【数 6 0】

$$x = (m0^{k_1} \oplus G(r)) || (r \oplus H(m0^{k_1} \oplus G(r)))$$

【 0 0 1 9 】

を計算する。さらに、

【 0 0 2 0 】

【数 6 1】

$$C = x^{2n\alpha} \bmod n$$

【 0 0 2 1 】

を計算し、さらに Jacobi 記号 $a = (x/n)$ を計算し、 (C, a) を暗号文として前記受信者側装置に送信する。

【0022】

[復号化]

受信者側装置は、受信者の秘密鍵 (p, q, β) を用いて、暗号文 (C, a) から、

【0023】

【数62】

$$\begin{aligned} x_{1,p} &= C^{\frac{(p+1)3q^{-1}}{4}} \bmod p, \\ x_{1,q} &= C^{\frac{(q+1)3p^{-1}}{4}} \bmod q \end{aligned}$$

【0024】

を計算し、 $\phi(x_{1,p}, x_{1,q})$, $\phi(-x_{1,p}, x_{1,q})$, $\phi(x_{1,p}, -x_{1,q})$,
 $\phi(-x_{1,p}, -x_{1,q})$ のうち、 $(y/n)=a$ かつ $0 < y < 2^{k-2}$ を満たす y を計算する。但し、 ϕ
 は中国人の剰余定理による

$Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。さらに、

【0025】

【数63】

$$y = s || t \quad (s \in \{0, 1\}^{k-k_0-2}, t \in \{0, 1\}^{k_0})$$

【0026】

とするとき、

【0027】

【数64】

$$z = G(H(s) \oplus t) \oplus s,$$

【0028】

を計算し、

【0029】

【数65】

$$m = \begin{cases} [z]^l & \text{if } [z]_{k_1} = 0^{k_1} \\ \text{"reject"} & \text{otherwise} \end{cases}$$

【 0 0 3 0 】

により、平文 m の復号化を行う。但し、 $[a]^k, [a]_k$ は各々 a の上位および下位 k ビットを表す。

【 0 0 3 1 】

【発明の実施の形態】

以下、図面を用いて、本発明の実施例について説明する。

【 0 0 3 2 】

図1は、本発明の実施例のシステム構成を示す図である。このシステムは、送信者側装置100と受信者側装置200から構成されている。さらに、送信者側装置100と受信者側装置200は通信回線300で接続されている。

【 0 0 3 3 】

図2は、実施例における送信者側装置100の内部構成を示す。送信者側装置100は、乱数生成手段101、べき乗算手段102、演算手段103、剰余演算手段104、メモリ105、通信装置106、入力装置107、を備えている。

【 0 0 3 4 】

図3は、実施例における受信者側装置200の内部構成を示す。受信者側装置200は、鍵生成手段201、べき乗算手段202、剰余演算手段203、演算手段204、メモリ205、通信装置206、を備えている。

【 0 0 3 5 】

図4は、実施例における計算機能付き記憶媒体400の内部構成を示す。計算機能付き記憶媒体400は、べき乗算器401、剰余演算器402、演算装置403、メモリ404、出力装置405、平文作成器406、乱数発生器407を備えている。

【 0 0 3 6 】

送信者側装置100、受信者側装置200、計算機能付き記憶媒体400は、いずれもCPUとメモリとを備えた計算機を用いて構成することができる。また、乱数生成手段、鍵生成手段、べき乗算手段、剰余演算手段、平文作成器、乱数発生器はいずれも専用のハードウェアを用いても良いし、演算手段上(CPU)上で動作するプログラムとして構成しても良い。各プログラムは、可搬型記憶媒体や通信回線上の通信媒体といった計算機が読みとり可能な媒体上に具現化され、これらの媒体を

介して計算機のメモリに格納される。

【 0 0 3 7 】

図5は、実施例1の概要を示す図である。

【 0 0 3 8 】

図6は、実施例6の概要を示す図である。

【 0 0 3 9 】

図7は、実施例7の概要を示す図である。

【 0 0 4 0 】

図8は、実施例9の概要を示す図である。

【 0 0 4 1 】

図9は、実施例11の概要を示す図である。

【 0 0 4 2 】

図10は、本発明の実施例11による方式と代表的な実用的公開鍵暗号方式との効率性(モジュラー積の個数)および安全性の比較を表す図である。図10における比較では、実施例11の方式において $\alpha = \beta = 1$ とした。なお、図10におけるデータの多くは、文献9(「従来の技術」に記載)から引用したものである。

(実施例 1)

本実施例は、メッセージの送信者であるAが受信者であるBに対して、送信データmを暗号通信によって送信する場合について説明する。

図1は、本実施例のシステム構成を示す。また、図5は、本実施例の概要を示す。

【 0 0 4 3 】

1. 鍵生成処理

受信者Bは、予め、受信者側装置200内の鍵生成手段201を用いて、

【 0 0 4 4 】

【数 6 6】

- p, q : 素数, $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【0045】

なる秘密情報(p, q, β)を作成し、

【0046】

【数67】

- $n = p^d q$ ($d > 1$ は奇数)
- k : pq のビット長
- $\alpha \in \mathbb{Z}$

【0047】

なる公開情報(n, k, α)を作成し(但し、 k は pq のビット長)、公開情報を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、例えば第3者(公開情報管理機関)への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ205に格納する。

【0048】

2. 暗復号化处理

(1)送信者Aは、平文 $m(0 < m < 2^{k-2})$ に対して、演算手段103、べき乗算手段102、剰余演算手段104を用いて、

【0049】

【数68】

$$C = m^{2\alpha} \bmod n$$

【0050】

を計算する。

【0051】

さらに、第3者あるいは受信者Bから上記公開情報を得て、演算手段103を用いて、Jacobi記号 $a = (m/n)$ を計算する(Jacobi記号の定義および計算方法については、例えば文献「高木貞治：初等整数論講義、岩波書店」に記載されている。)。

【0052】

さらに、暗号文(C, a)を通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【 0 0 5 3 】

(2)受信者Bは、保持している上記秘密情報 (p, q, β) と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文 (C, a) から、

【 0 0 5 4 】

【数 6 9】

$$m_{1,p} = C^{\frac{(p+1)3q-1}{4}} \bmod p,$$

$$m_{1,q} = C^{\frac{(q+1)3p-1}{4}} \bmod q$$

【 0 0 5 5 】

を計算し、 $\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たすものを平文 m とする。但し、 ϕ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。

【 0 0 5 6 】

上記公開鍵暗号方法において、 $\alpha = \beta = 1$ と固定して、 α, β の各々を公開鍵、秘密鍵から削除することで、本実施例の方法における鍵情報を短縮することが可能となる。

【 0 0 5 7 】

また、秘密鍵 p, q は、素数 p', q' から $p=2p'+1, q=2q'+1$ により作成することも可能である。

【 0 0 5 8 】

本実施例の公開鍵暗号方法においては、 $d (d > 1)$ の値はシステムにより可変とする。これにより、平文 m のビット長が常に小さい場合、 n の素因数分解が困難である範囲において d の値を大きくすることにより、復号化処理を高速にすることが可能である。

【 0 0 5 9 】

本実施例による方法では、例えば $d=3$ の場合、 n の素因数分解問題の困難性を前提として完全解読が不可能なことを示すことができる。すなわち、 n の素因数分解問題を解くアルゴリズムが存在すれば、そのアルゴリズムを利用して本実施

例の方法の完全解読を行うアルゴリズムを構成することができる。また、本実施例の方法の完全解読を行うアルゴリズムが存在すれば、そのアルゴリズムを利用して、 n の素因数分解問題を解くアルゴリズムを構成することができる。

【0060】

(実施例 2)

本実施例は、実施例1においては暗号文の一部としている a を公開鍵とする場合について述べる。

図1は、本実施例のシステム構成を示す。

1. 鍵生成処理

受信者Bは、予め、受信者側装置200内の鍵生成手段201を用いて、

【0061】

【数70】

- p, q : 素数, $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【0062】

なる秘密情報(p, q, β)を作成し、

【0063】

【数71】

- $n = p^d q$ ($d > 1$ は奇数)
- k : pq のビット長
- $\alpha \in \mathbb{Z}$
- $a \in \{-1, 1\}$

【0064】

なる公開情報(n, k, α, a)を作成し(但し、 k は pq のビット長)、公開情報を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、例えば第3者(公開情報管理機関)への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ205に格納する。

【0065】

2. 暗復号化处理

(1)送信者Aは、 $a=(m/n)$ なる平文 $m(0<m<2^{k-2})$ に対して、演算手段103、べき乗算手段102、剰余演算手段104を用いて、

【0066】

【数72】

$$C = m^{2n\alpha} \bmod n$$

【0067】

を計算する。

【0068】

さらに、暗号文Cを通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【0069】

(2)受信者Bは、保持している上記秘密情報 (p, q, β) と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文Cから、

【0070】

【数73】

$$\begin{aligned} m_{1,p} &= C^{\frac{(p+1)\beta q^{-1}}{4}} \bmod p, \\ m_{1,q} &= C^{\frac{(q+1)\beta p^{-1}}{4}} \bmod q \end{aligned}$$

【0071】

を計算し、 $\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0<x<2^{k-2}$ を満たすものを平文 m とする。但し、 ϕ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。

【0072】

上記公開鍵暗号方法において、 $\alpha = \beta = 1$ と固定して、 α, β の各々を公開鍵、秘密鍵から削除することで、本実施例の方法における鍵情報を短縮することが

可能となる。

【0073】

また、秘密鍵 p, q は、素数 p', q' から $p=2p'+1$, $q=2q'+1$ により作成することも可能である。

【0074】

本実施例の公開鍵暗号方法においては、 $d (d > 1)$ の値はシステムにより可変とする。これにより、平文 m のビット長が常に小さい場合、 n の素因数分解が困難である範囲において d の値を大きくすることにより、復号化処理を高速にすることが可能である。

【0075】

(実施例 3)

本実施例は、実施例1および2において、送信者が受信者に対し送信したいメッセージ文に対して、正しく復号されたかを確認するための検査情報を含むように平文 m を作成する方法について述べる。実施例1および2の公開鍵暗号方法は、選択平文攻撃に対して、一方向であることが証明できるが、選択暗号文攻撃に対しては安全ではない。そこで、送信者が受信者に対し送信したいメッセージ文に対して、予め定められた冗長性を持たせた内容を平文 m とし、実施例1(または実施例2)の方法により暗号化し、受信者は実施例1(または実施例2)の方法により平文 m を復号化し、予め定められた冗長性を確認する(もし、予め定められた冗長性を持たない場合は、復号が正しく行われなかったものとみなす。)。

【0076】

他の方法としては、送信者が受信者に対し送信したいメッセージ文に対して、予め定められた意味のあるメッセージを加えた内容を平文 m とし、実施例1(または実施例2)の方法により暗号化し、受信者は実施例1(または実施例2)の方法により平文 m を復号化し、予め定められた意味のあるメッセージの内容を確認する(もし、予め定められた意味のあるメッセージの内容が一致しない場合は、復号が正しく行われなかったものとみなす。)。

【0077】

このような方法により、実施例1および実施例2の公開鍵暗号方式は、選択暗号

文攻撃に対しても、ある程度の安全性を確保することができる(選択暗号文攻撃に対して安全性が証明できる方法については、実施例で述べる)。

【 0 0 7 8 】

(実施例 4)

本実施例は、受信者が作成した公開情報を用いて、送信者と受信者の2者間で同一の値を共有するための鍵共有方法について述べる。

【 0 0 7 9 】

1. 鍵生成処理

受信者 B は、予め、受信者側装置200内の鍵生成手段201を用いて、

【 0 0 8 0 】

【数 7 4】

- p, q : 素数, $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【 0 0 8 1 】

なる秘密情報 (p, q, β) を作成し、

【 0 0 8 2 】

【数 7 5】

- $n = p^d q$ ($d > 1$ は奇数)
- k : pq のビット長
- $\alpha \in \mathbb{Z}$
- f : 一方向性関数

【 0 0 8 3 】

なる公開情報 (n, k, α, f) を作成し(但し、 k は pq のビット長)、公開情報を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、例えば第3者(公開情報管理機関)への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ205に格納する。

【 0 0 8 4 】

2. 鍵配送処理

(1)送信者 A は、平文 $m(0 < m < 2^{k-2})$ に対して、演算手段103、べき乗算手段102、剰

余演算手段104を用いて、

【0085】

【数76】

$$C = m^{2n\alpha} \bmod n$$

【0086】

を計算する。

【0087】

さらに、第3者あるいは受信者Bから上記公開情報を得て、演算手段103を用いて、Jacobi記号 $a=(m/n)$ を計算する。

【0088】

さらに、暗号文 (C, a) を通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【0089】

また、送信者は、公開情報である一方向性関数 f から、演算手段103、剰余演算手段104を用いて、共有鍵 $K=f(m)$ を計算する。

【0090】

(2)受信者Bは、保持している上記秘密情報 (p, q, β) と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文 (C, a) から、

【0091】

【数77】

$$m_{1,p} = C^{\frac{(p+1)\beta q^{-1}}{4}} \bmod p,$$

$$m_{1,q} = C^{\frac{(q+1)\beta p^{-d}}{4}} \bmod q$$

【0092】

を計算し、 $\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たすものを平文 m とする(但し、 ϕ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す)。さらに、受信者Bは公開情報である一方向性関数 f から、演算手段204を用い

て共有鍵 $K=f(m)$ を計算する。

【0093】

上記公開鍵配送方法において、 $\alpha = \beta = 1$ と固定して、 α 、 β の各々を公開鍵、秘密鍵から削除することで、本実施例の方法における鍵情報を短縮することが可能となる。

【0094】

また、秘密鍵 p, q は、素数 p', q' から $p=2p'+1$, $q=2q'+1$ により作成することも可能である。

【0095】

本実施例の公開鍵暗号方法においては、 $d (d > 1)$ の値はシステムにより可変とする。これにより、平文 m のビット長が常に小さい場合、 n の素因数分解が困難である範囲において d の値を大きくすることにより、復号化処理を高速にすることが可能である。

【0096】

(実施例 5)

本実施例は、実施例4においては暗号文の一部としている a を公開鍵とする場合について述べる。

【0097】

1. 鍵生成処理

受信者Bは、予め、受信者側装置200内の鍵生成手段201を用いて、

【0098】

【数 7 8】

- p, q : 素数, $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【0099】

なる秘密情報 (p, q, β) を作成し、

【0100】

【数79】

- $n = p^d q$ ($d > 1$ は奇数)
- k : pq のビット長
- $\alpha \in \mathbb{Z}$
- $a \in \{-1, 1\}$
- f : 一方方向性関数

【0101】

なる公開情報(n, k, α, a, f)を作成し(但し, k は pq のビット長), 公開情報を通信回線300などを介して出力し, 送信者側装置100へ送付するか, または公開する。公開する方法として, 例えば第3者(公開情報管理機関)への登録など, 周知の方法を用いることが可能である。その他の情報については, メモリ205に格納する。

【0102】

2. 鍵配送処理

(1)送信者Aは, $a=(m/n)$ なる平文 $m(0 < m < 2^{k-2})$ に対して(但し, $a=(m/n)$ はJacobi記号を表す), 演算手段103, べき乗算手段102, 剰余演算手段104を用いて,

【0103】

【数80】

$$C = m^{2n\alpha} \bmod n$$

【0104】

を計算する。

【0105】

さらに, 暗号文Cを通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【0106】

また, 送信者は, 公開情報である一方方向性関数 f から, 演算手段103, 剰余演算手段104を用いて, 共有鍵 $K=f(m)$ を計算する。

【 0 1 0 7 】

(2)受信者Bは、保持している上記秘密情報 (p, q, β) と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文Cから、

【 0 1 0 8 】

【数 8 1】

$$m_{1,p} = C^{\frac{(p+1)2q^{-1}}{4}} \bmod p,$$

$$m_{1,q} = C^{\frac{(q+1)2p^{-1}}{4}} \bmod q$$

【 0 1 0 9 】

を計算し、 $\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たすものを平文 m とする(但し、 ϕ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。)。さらに、受信者Bは公開情報である一方向性関数 f から、演算手段204を用いて共有鍵 $K=f(m)$ を計算する。

【 0 1 1 0 】

上記公開鍵配送方法において、 $\alpha = \beta = 1$ と固定して、 α , β の各々を公開鍵、秘密鍵から削除することで、本実施例の方法における鍵情報を短縮することが可能となる。

【 0 1 1 1 】

また、秘密鍵 p, q は、素数 p', q' から $p=2p'+1$, $q=2q'+1$ により作成することも可能である。

【 0 1 1 2 】

また、本実施例の公開鍵暗号方法においては、 d ($d > 1$)の値はシステムにより可変とする。これにより、平文 m のビット長が常に小さい場合、 n の素因数分解が困難である範囲において d の値を大きくすることにより、復号化処理を高速にすることが可能である。

(実施例 6)

本実施例は、実施例1から実施例5において、ICカードのような計算能力の小さな計算機能付き記憶媒体400が計算能力の高い送信者側装置100を利用して、暗号

文Cを計算する方法について述べる。図6は、本実施例の概要を示す。

【0113】

計算機能付き記憶媒体400は、平文作成器406を用いて、平文 $m(0 < m < 2^{k-2})$ を作成する。さらに、計算機能付き記憶媒体400は、公開鍵 α 、 n から、べき乗算器401、剰余演算器402を用いて、

【0114】

【数82】

$$C_1 = m^{2\alpha} \bmod n$$

【0115】

を計算し、出力装置405から、送信者側装置100の入力装置107に出力する。

【0116】

送信者側装置100は、べき乗算手段202、剰余演算手段203を用いて、暗号文Cを、

【0117】

【数83】

$$C = C_1^n \bmod n$$

【0118】

にて計算する。

【0119】

(実施例 7)

本実施例は、文献12(「従来の技術」で記述)に記載されている変換方法により、実施例1の公開鍵暗号方法を、適応的選択暗号文攻撃に対して強秘匿であることが証明可能な公開鍵暗号方法へ転換する。

【0120】

図1は、本実施例のシステム構成を示す。また、図7は、本実施例の概要を示す。

【 0 1 2 1 】

1. 鍵生成処理

受信者 B は、予め、受信者側装置 200 内の鍵生成手段 201 を用いて、

【 0 1 2 2 】

【数 8 4】

- p, q : 素数, $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【 0 1 2 3 】

なる秘密情報 (p, q, β) を作成し、

【 0 1 2 4 】

【数 8 5】

- $n = p^d q$ ($d > 1$ は奇数)
- k, k_0, k_1 : k は pq のビット長, k_0, k_1 は $k > k_0 - k_1 - 2$ なる正整数
- $\alpha \in \mathbb{Z}$
- $G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k-k_0-2}$
- $H : \{0, 1\}^{k-k_0-2} \rightarrow \{0, 1\}^{k_0}$

【 0 1 2 5 】

なる公開情報 $(n, k, k_0, k_1, \alpha, G, H)$ を作成し (但し, k は p, q のビット長を表す。) , 公開情報を通信回線 300 などを介して出力し, 送信者側装置 100 へ送付するか, または公開する。公開する方法として, 例えば第 3 者 (公開情報管理機関) への登録など, 周知の方法を用いることが可能である。その他の情報については, メモリ 205 に格納する。

【 0 1 2 6 】

2. 暗復号化処理

(1) 送信者 A は, 平文 $m (m \in \{0, 1\}^l, l = k - k_0 - k_1 - 2)$ に対して, 乱数生成手段 101 を用いて乱数 $r (r \in \{0, 1\}^{k_0})$ を選び, さらに演算手段 103 を用いて,

【 0 1 2 7 】

【数 8 6】

$$x = (m0^{k_1} \oplus G(r)) || (r \oplus H(m0^{k_1} \oplus C(r)))$$

【 0 1 2 8 】

を計算し、さらに、演算手段103、べき乗算手段102、剰余演算手段104を用いて

【 0 1 2 9 】

【数 8 7】

$$C = x^{2na} \bmod n$$

【 0 1 3 0 】

を計算する。

【 0 1 3 1 】

さらに、第3者あるいは受信者Bから上記公開情報を得て、演算手段103を用いて、Jacobi記号 $a=(x/n)$ を計算する。

【 0 1 3 2 】

さらに、暗号文 (C, a) を通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【 0 1 3 3 】

(2)受信者Bは、保持している上記秘密情報 (p, q, β) と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文 (C, a) から、

【 0 1 3 4 】

【数 8 8】

$$x_{1,p} = C^{\frac{(p+1)3q^{-1}}{4}} \bmod p,$$

$$x_{1,q} = C^{\frac{(q+1)3p^{-1}}{4}} \bmod q$$

【 0 1 3 5 】

を計算し、 $\phi(x_{1,p}, x_{1,q}), \phi(-x_{1,p}, x_{1,q}), \phi(x_{1,p}, -x_{1,q}),$

$\phi(-x_{1,p}, -x_{1,q})$ のうち、 $(y/n)=a$ かつ $0 < y < 2^{k-2}$ を満たす y を計算する。但し、 ϕ は中国人の剰余定理による

$\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ から $\mathbb{Z}/(pq)$ への環同型写像を表す。

【0 1 3 6】

さらに、

【0 1 3 7】

【数 8 9】

$$y = s||t \quad (s \in \{0, 1\}^{k-k_0-2}, t \in \{0, 1\}^{k_0})$$

【0 1 3 8】

とするとき、演算手段204を用いて

【0 1 3 9】

【数 9 0】

$$z = G(H(s) \oplus t) \oplus s,$$

【0 1 4 0】

を計算し、

【0 1 4 1】

【数 9 1】

$$m = \begin{cases} [z]^l & \text{if } [z]_{k_1} = 0^{k_1} \\ \text{"reject"} & \text{otherwise} \end{cases}$$

【0 1 4 2】

により、平文 m の復号化を行う。但し、 $[a]^k, [a]_k$ は各々 a の上位および下位 k ビットを表す。

【0 1 4 3】

上記方法を用いれば、例えば $d=3$ の場合、適応的選択暗号文攻撃に対して強秘匿であることが n の素因数分解問題の困難性との等価性により証明することができる(文献12において、一般的な落し戸付き置換を対象に証明されている。)

【0 1 4 4】

また、本実施例の方法によると、復号化処理において、 n よりも小さい pq を法とする剰余環から決定される乗法群の上で行うことにより、従来方法に比べて処理の高速性を実現している。

【0 1 4 5】

上記公開鍵暗号方法において、 $\alpha = \beta = 1$ と固定して、 α 、 β の各々を公開鍵、秘密鍵から削除することで、本実施例の方法における鍵情報を短縮することが可能となる。

【0 1 4 6】

また、秘密鍵 p, q は、素数 p', q' から $p = 2p' + 1$, $q = 2q' + 1$ により作成することも可能である。

【0 1 4 7】

本実施例の公開鍵暗号方法においては、 d ($d > 1$)の値はシステムにより可変とする。これにより、平文 m のビット長が常に小さい場合、 n の素因数分解が困難である範囲において d の値を大きくすることにより、復号化処理を高速にすることが可能である。

【0 1 4 8】

(実施例 8)

本実施例は、実施例7においては暗号文の一部としている a を公開鍵とする場合について述べる。図1は、本実施例のシステム構成を示す。

1. 鍵生成処理

受信者Bは、予め、受信者側装置200内の鍵生成手段201を用いて、

【0 1 4 9】

【数 9 2】

- p, q : 素数, $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$
- $3 \in \mathbb{Z}$, $\alpha 3 \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【0 1 5 0】

なる秘密情報 (p, q, β) を作成し、

【0151】

【数93】

- $n = p^d q$ ($d > 1$ は奇数)
- $k, k_0, k_1 \in \mathbb{Z}$: k は pq のビット長, k_0, k_1 は $k > k_0 - k_1 - 2$ なる正整数
- $\alpha \in \mathbb{Z}$
- $a \in \{-1, 1\}$
- $G: \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k-k_0-2}$
- $H: \{0, 1\}^{k-k_0-2} \rightarrow \{0, 1\}^{k_0}$

【0152】

なる公開情報 $(n, k, k_0, k_1, \alpha, a, G, H)$ を作成し, 公開情報を通信回線300などを介して出力し, 送信者側装置100へ送付するか, または公開する。公開する方法として, 例えば第3者(公開情報管理機関)への登録など, 周知の方法を用いることが可能である。その他の情報については, メモリ205に格納する。

【0153】

2. 暗復号化处理

(1)送信者Aは, 平文 $m (m \in \{0, 1\}^l, l = k - k_0 - k_1 - 2)$ に対して, 乱数生成手段101を用いて乱数 $r (r \in \{0, 1\}^{k_0})$ を選び, さらに演算手段103を用いて, $a = (x/n)$ なる

【0154】

【数94】

$$x = (m0^{k_1} \oplus G(r)) || (r \oplus H(m0^{k_1} \oplus G(r)))$$

【0155】

を計算し, さらに, 演算手段103, べき乗算手段102, 剰余演算手段104を用いて

【0156】

【数95】

$$C = x^{2n\alpha} \bmod n$$

【0157】

を計算する。

【 0 1 5 8 】

さらに、第3者あるいは受信者Bから上記公開情報を得て、演算手段103を用いて、Jacobi記号 $a=(x/n)$ を計算する。

【 0 1 5 9 】

さらに、暗号文Cを通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【 0 1 6 0 】

(2)受信者Bは、保持している上記秘密情報 (p, q, β) と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文Cから、

【 0 1 6 1 】

【数 9 6】

$$\begin{aligned} x_{1,p} &= C^{\frac{(p+1)\beta q^{-1}}{4}} \bmod p, \\ x_{1,q} &= C^{\frac{(q+1)\beta p^{-1}}{4}} \bmod q \end{aligned}$$

【 0 1 6 2 】

を計算し、 $\phi(x_{1,p}, x_{1,q}), \phi(-x_{1,p}, x_{1,q}), \phi(x_{1,p}, -x_{1,q}), \phi(-x_{1,p}, -x_{1,q})$ のうち、 $(y/n)=a$ かつ $0 < y < 2^{k-2}$ を満たす y を計算する。但し、 ϕ は中国人の剰余定理による

$Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。

【 0 1 6 3 】

さらに、

【 0 1 6 4 】

【数 9 7】

$$y = s||t \quad (s \in \{0, 1\}^{k-k_0-2}, t \in \{0, 1\}^{k_0})$$

【 0 1 6 5 】

とすると、演算手段204を用いて

【 0 1 6 6 】

【数 9 8】

$$z = G(H(s) \oplus t) \oplus s,$$

【 0 1 6 7 】

を計算し、

【 0 1 6 8 】

【数 9 9】

$$m = \begin{cases} [z]^t & \text{if } [z]_{k_1} = 0^{k_1} \\ \text{"reject"} & \text{otherwise} \end{cases}$$

【 0 1 6 9 】

により、平文 m の復号化を行う。但し、 $[a]^k, [a]_k$ は各々 a の上位および下位 k ビットを表す。

【 0 1 7 0 】

上記公開鍵暗号方法において、 $\alpha = \beta = 1$ と固定して、 α, β の各々を公開鍵、秘密鍵から削除することで、本実施例の方法における鍵情報を短縮することが可能となる。

【 0 1 7 1 】

また、秘密鍵 p, q は、素数 p', q' から $p=2p'+1, q=2q'+1$ により作成することも可能である。

【 0 1 7 2 】

本実施例の公開鍵暗号方法においては、 $d (d > 1)$ の値はシステムにより可変とする。これにより、平文 m のビット長が常に小さい場合、 n の素因数分解が困難である範囲において d の値を大きくすることにより、復号化処理を高速にすることが可能である。

【 0 1 7 3 】

(実施例 9)

本実施例は、実施例7および実施例8において、ICカードのような計算能力の小

さな計算機能付き記憶媒体400が計算能力の高い送信者側装置100を利用して、暗号文Cを計算する方法について述べる。図8は、本実施例の概要を示す。

【0 1 7 4】

計算機能付き記憶媒体400は、平文作成器406を用いて、平文 $m(m \in \{0,1\}^l, l=k-k_0-k_1-2)$ を作成する。さらに、乱数発生器407を用いて乱数 $r(r \in \{0,1\}^{k_0})$ を作成し、演算装置403を用いて、関数 G, H から、

【0 1 7 5】

【数 1 0 0】

$$x = (m0^{k_1} \oplus G(r)) || (r \oplus H(m0^{k_1} \oplus G(r)))$$

【0 1 7 6】

を計算する。さらに、計算機能付き記憶媒体400は、公開鍵 α , n から、べき乗算器401、剰余演算器402を用いて、

【0 1 7 7】

【数 1 0 1】

$$C_1 = x^{2\alpha} \bmod n$$

【0 1 7 8】

を計算し、出力装置405から、送信者側装置100の入力装置107に出力する。

【0 1 7 9】

送信者側装置100は、べき乗算手段202、剰余演算手段203を用いて、暗号文Cを、

【0 1 8 0】

【数 1 0 2】

$$C = C_1^n \bmod n$$

【0 1 8 1】

にて計算する。

【 0 1 8 2 】

(実施例 10)

本実施例では、実施例1から実施例5および実施例7、実施例8の公開鍵暗号化方法の変形例であって、安全性の証明を与えることはできないが、暗号化及び復号化処理の効率性に優れた公開鍵暗号化方法について述べる。以下、前述の実施例に沿って、変更部分のみを記述する。

【 0 1 8 3 】

実施例1から実施例5において、送信者側装置100内の演算手段103を用いて、暗号文Cを、

【 0 1 8 4 】

【数 1 0 3】

$$C = m^{2\alpha} \bmod n$$

【 0 1 8 5 】

にて計算する。

【 0 1 8 6 】

また、実施例1から5において、 $m_{1,p}$ および $m_{1,q}$ を、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文Cから、

【 0 1 8 7 】

【数 1 0 4】

$$\begin{aligned} m_{1,p} &= C^{\frac{(p+1)s}{4}} \bmod p, \\ m_{1,q} &= C^{\frac{(q+1)s}{4}} \bmod q \end{aligned}$$

【 0 1 8 8 】

にて計算する。

【 0 1 8 9 】

実施例7から実施例8においては、送信者側装置100内の演算手段103を用いて、暗号文Cを、

【0 1 9 0】

【数 1 0 5】

$$C = x^{2\alpha} \bmod n$$

【0 1 9 1】

また、実施例7から8において、 $m_{1,p}$ および $m_{1,q}$ を、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文Cから、
にて計算する。

【0 1 9 2】

【数 1 0 6】

$$m_{1,p} = C^{\frac{(p+1)s}{4}} \bmod p,$$

$$m_{1,q} = C^{\frac{(q+1)s}{4}} \bmod q$$

【0 1 9 3】

にて計算する。

【0 1 9 4】

(実施例 11)

本実施例では、実施例7および実施例8において、識別情報 a を省略する場合
について述べる。

【0 1 9 5】

この場合、送信者Aは、平文 $m(m \in \{0,1\}^l, l=k-k_0-k_1-2)$ に対して、乱数生成手段101を用いて乱数 $r(r \in \{0,1\}^{k_0})$ を選び、さらに演算手段103を用いて

【0 1 9 6】

【数 1 0 7】

$$x = (m0^{k_1} \oplus G(r)) || (r \oplus H(m0^{k_1} \oplus G(r)))$$

【0 1 9 7】

を計算し、さらに、演算手段103、べき乗算手段102、剰余演算手段104を用いて

【0198】

【数108】

$$C = x^{2n\alpha} \bmod n$$

【0199】

を計算する。さらに、暗号文Cを通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【0200】

受信者Bは、保持している上記秘密情報(p,q,β)と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文Cから、

【0201】

【数109】

$$\begin{aligned} x_{1,p} &= C^{\frac{(p+1)3q^{-1}}{4}} \bmod p, \\ x_{1,q} &= C^{\frac{(q+1)3p^{-1}}{4}} \bmod q \end{aligned}$$

【0202】

を計算し、各 $y_1 = \phi(x_{1,p}, x_{1,q})$, $y_2 = \phi(-x_{1,p}, x_{1,q})$, $y_3 = \phi(x_{1,p}, -x_{1,q})$, $y_4 = \phi(-x_{1,p}, -x_{1,q})$ に対して、

【0203】

【数110】

$$y_i = s_i || t_i \quad (s_i \in \{0,1\}^{k-k_0-2}, t_i \in \{0,1\}^{k_0}, 1 \leq i \leq 4)$$

【0204】

とするとき、演算手段204を用いて

【0205】

【数111】

$$z_i = G(H(s_i) \oplus t_i) \oplus s_i \quad (1 \leq i \leq 4),$$

【0206】

を計算し、

【0207】

【数112】

$$m = \begin{cases} [z_i]^l & \text{if } [z_i]_{k_1} = 0^{k_1} \\ \text{"reject"} & \text{otherwise} \end{cases}$$

【0208】

により、平文 m の復号化を行う。但し、 ϕ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。また、 $[a]^k, [a]_k$ は各々 a の上位および下位 k ビットを表す

(実施例 12)

本実施例は、文献4に記載の公開鍵暗号化方法に、文献12に記載の変換方法を施し、さらに復号化処理の効率性を向上させた公開鍵暗号方法について述べる。

図1は、本実施例のシステム構成を示す。図9は、本実施例の概要を示す。

【0209】

1. 鍵生成処理

受信者Bは、予め、受信者側装置200内の鍵生成手段201を用いて、

【0210】

【数113】

- p_i : 素数 ($p_i \equiv 3 \pmod{4}$, $1 \leq i \leq h$)
- $\beta \in \mathbb{Z}$, $\alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【0211】

なる秘密情報 (p_i, β) ($1 \leq i \leq h$)を作成し、

【0 2 1 2】

【数 1 1 4】

- $n = \prod_{i=1}^h p_i$
- $k, k_0, k_1 \in \mathbb{Z} : k$ は n のビット長, k_0, k_1 は $k > k_0 - k_1 - 2$ なる正整数
- $\alpha \in \mathbb{Z}$
- $G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k-k_0}$
- $H : \{0, 1\}^{k-k_0} \rightarrow \{0, 1\}^{k_0}$

【0 2 1 3】

なる公開情報 $(n, k, k_0, k_1, \alpha, G, H)$ を作成し, 公開情報を通信回線300などを介して出力し, 送信者側装置100へ送付するか, または公開する。公開する方法として, 例えば第3者(公開情報管理機関)への登録など, 周知の方法を用いることが可能である。その他の情報については, メモリ205に格納する。

【0 2 1 4】

2. 暗号化処理

送信者Aは, 平文 $m (m \in \{0, 1\}^l, l = k - k_0 - k_1 - 2)$ に対して, 乱数生成手段101を用いて乱数 $r (r \in \{0, 1\}^{k_0})$ を選び,

【0 2 1 5】

【数 1 1 5】

$$x = (m0^{k_1} \oplus G(r)) || (r \oplus H(m0^{k_1} \oplus G(r)))$$

【0 2 1 6】

を計算し, さらに, 第3者あるいは受信者Bから上記公開情報を得て, 演算手段103, べき乗算手段102, 剰余演算手段104を用いて,

【0 2 1 7】

【数 1 1 6】

$$C = x^{2\alpha} \bmod n$$

【0 2 1 8】

を計算する。

【 0 2 1 9 】

さらに、暗号文Cを通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【 0 2 2 0 】

3. 復号化处理

受信者Bは、保持している上記秘密情報 $(p_i, \beta) (1 \leq i \leq h)$ と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文Cから、

【 0 2 2 1 】

【数 1 1 7】

$$x_i = C^{\frac{(p_i+1)\beta}{4}} \bmod p_i$$

【 0 2 2 2 】

を計算し、 2^h 個の

$\{\phi(e_1x_1, e_2x_2, \dots, e_hx_h) | e_1, \dots, e_h \in \{-1, 1\}\}$ について、

【 0 2 2 3 】

【数 1 1 8】

$$y_i = s_i || t_i \quad (s_i \in \{0, 1\}^{k-k_0}, t_i \in \{0, 1\}^{k_0}, 1 \leq i \leq 2^h)$$

【 0 2 2 4 】

とするとき、演算手段204を用いて、

【 0 2 2 5 】

【数 1 1 9】

$$z_i = G(H(s_i) \oplus t_i) \oplus s_i \quad (1 \leq i \leq 2^h)$$

【 0 2 2 6 】

を計算し、

【0227】

【数120】

$$m = \begin{cases} [z_i]^l & \text{if } [z_i]_{k_1} = 0^{k_1} \\ \text{"reject"} & \text{otherwise} \end{cases}$$

【0228】

により、平文 m の復号化を行う。但し、 ϕ は中国人の剰余定理による $Z/(p_1) \times Z/(p_2) \times \dots \times Z/(p_h)$ から $Z/(n)$ への環同型写像を表す。また、 $[a]^k, [a]_k$ は各々 a の上位および下位 k ビットを表す。

【0229】

上記公開鍵暗号方法において、 $\alpha = \beta = 1$ と固定して、 α, β の各々を公開鍵、秘密鍵から削除することで、本実施例の方法における鍵情報を短縮することが可能となる。

【0230】

また、 x と $n/2$ の大小関係、または、Jacobi記号 (x/n) の値、等の識別情報を暗号文と共に送信する(または、公開情報により指定された識別情報の通りに、 x を作成する)ことにより、 2^h 個の $\{\phi(e_1x_1, e_2x_2, \dots, e_hx_h) \mid e_1, \dots, e_h \in \{-1, 1\}\}$ から正しい平文を復号化する際の効率化向上を行うことができる。

【0231】

本実施例による方法では、従来方式である文献4に記載の公開鍵暗号方法では、公開鍵の一部である n が3個以上の相異なる素数の積であった場合、安全性の証明が可能であることを前提に、一意復号を行うことが難しかった問題を解決している。

【0232】

以上、実施例では、送信者と受信者が各々の装置を利用して暗号通信を行うという一般形で述べたが、具体的には様々なシステムに適用される。

【0233】

例えば、電子ショッピングシステムでは、送信者はユーザであり、送信者側装

置はパソコンなどの計算機であり、受信者は小売店、受信者側装置はパソコンなどの計算機となる。このとき、ユーザの商品等の注文書は共通鍵暗号で暗号化されることが多く、その際の暗号化鍵を本実施例による方法により暗号化されて小売店側装置に送信される。

【 0 2 3 4 】

また、電子メールシステムでは、各々の装置はパソコンなどの計算機であり、送信者のメッセージは共通鍵暗号で暗号化されることが多く、その際の暗号化鍵を本実施例による方法により暗号化されて受信者の計算機に送信される。

【 0 2 3 5 】

その他にも、従来の公開鍵暗号が使われている様々なシステムに適用することが可能である。

【 0 2 3 6 】

なお、本実施例における各計算は、CPUがメモリ内の各プログラムを実行することにより行われるものとして説明したが、プログラムだけではなく、いずれかがハードウェア化された演算装置であって、他の演算装置や、CPUと、データのやりとりを行うものであっても良い。

【 0 2 3 7 】

【発明の効果】

本発明によれば、選択平文攻撃、また、最も強力な攻撃法である適応的選択暗号文攻撃に対しても安全であり、さらに、高速処理が可能な、公開鍵暗号方法並びに鍵共有方法と、その応用装置、システムを実現することができる。

【図面の簡単な説明】

【図 1】

本発明の実施例のシステム構成を示す図である。

【図 2】

本発明の実施例における送信者側装置の内部構成を示す図である。

【図 3】

本発明の実施例における受信者側装置の内部構成を示す図である。

【図 4】

本発明に実施例における計算機能付き記憶媒体の内部構成を示す図である。

【図 5】

本発明の実施例1の概要を示す図である。

【図 6】

本発明の実施例6の概要を示す図である。

【図 7】

本発明の実施例7の概要を示す図である。

【図 8】

本発明の実施例9の概要を示す図である。

【図 9】

本発明の実施例11の概要を示す図である。

【図 1 0】

本発明の実施例11($\alpha = \beta = 1$)による方式と代表的な実用的公開鍵暗号方式との効率性(モジュラー積の個数)および安全性の比較を示す図である。

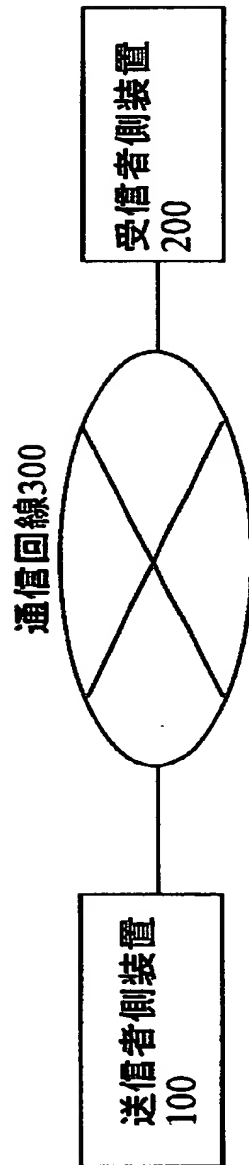
【符号の説明】

100…送信者側装置, 101…送信者側装置100内の乱数生成手段, 102…送信者側装置100内のべき乗算手段, 103…送信者側装置100内の演算手段, 104…送信者側装置100内の剰余演算手段, 105…送信者側装置100内のメモリ, 106…送信者側装置100内の通信装置, 107…送信者側装置100内の入力装置, 200…受信者側装置, 201…受信者側装置200内の鍵生成手段, 202…受信者側装置200内のべき乗算手段, 203…受信者側装置200内の剰余演算手段, 204…受信者側装置200内の演算手段, 205…受信者側装置200内のメモリ, 206…受信者側装置200内の通信装置, 300…通信回線, 400…計算機能付き記憶媒体, 401…計算機能付き記憶媒体400内のべき乗算器, 402…計算機能付き記憶媒体400内の剰余演算器, 403…計算機能付き記憶媒体400内の演算器, 404…計算機能付き記憶媒体400内のメモリ, 405…計算機能付き記憶媒体400内の出力装置, 406…計算機能付き記憶媒体400内の平文作成器, 407…計算機能付き記憶媒体400内の乱数生成器。

【書類名】 図面

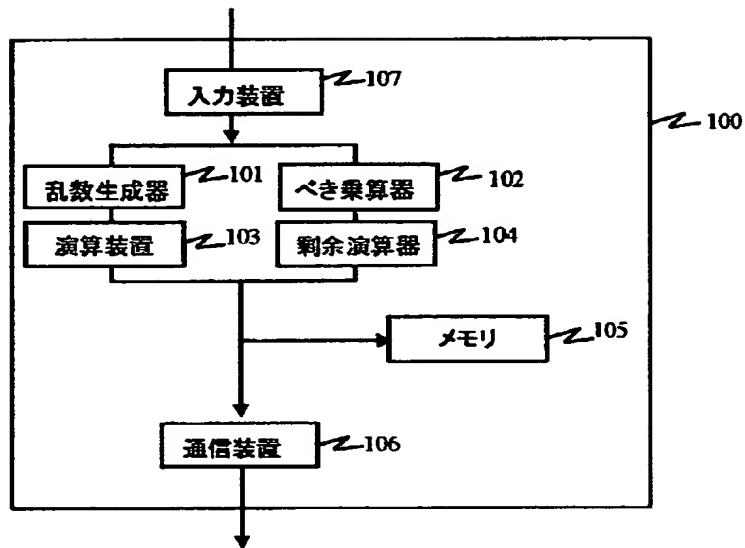
【図 1】

図 1



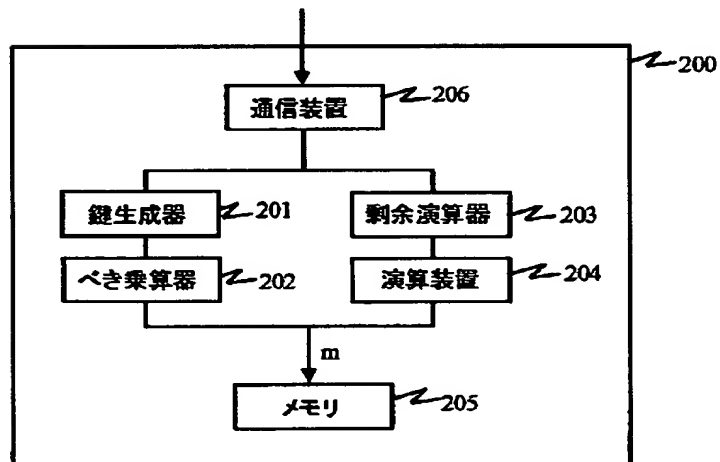
【図 2】

図 2

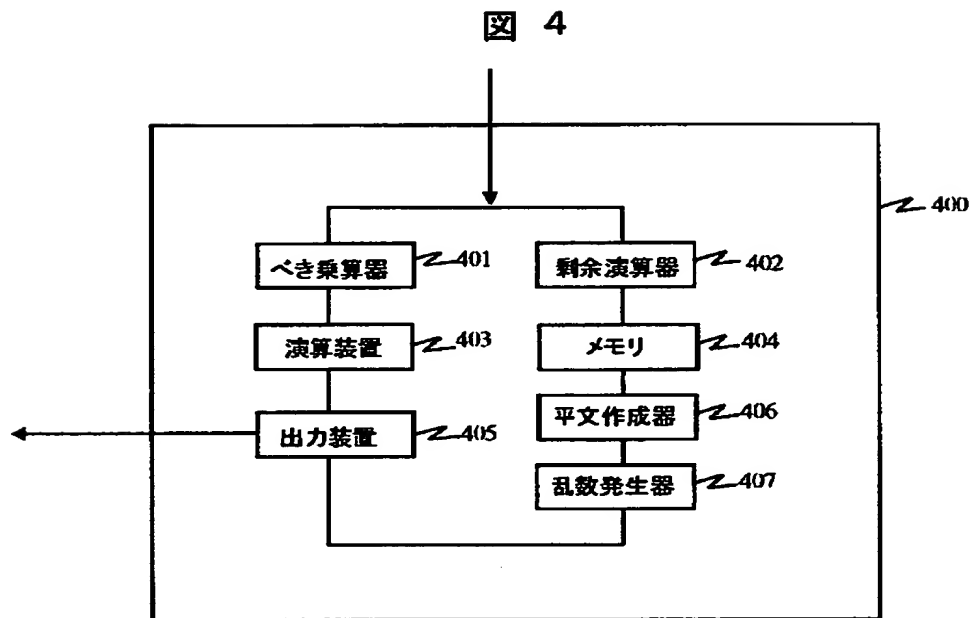


【図 3】

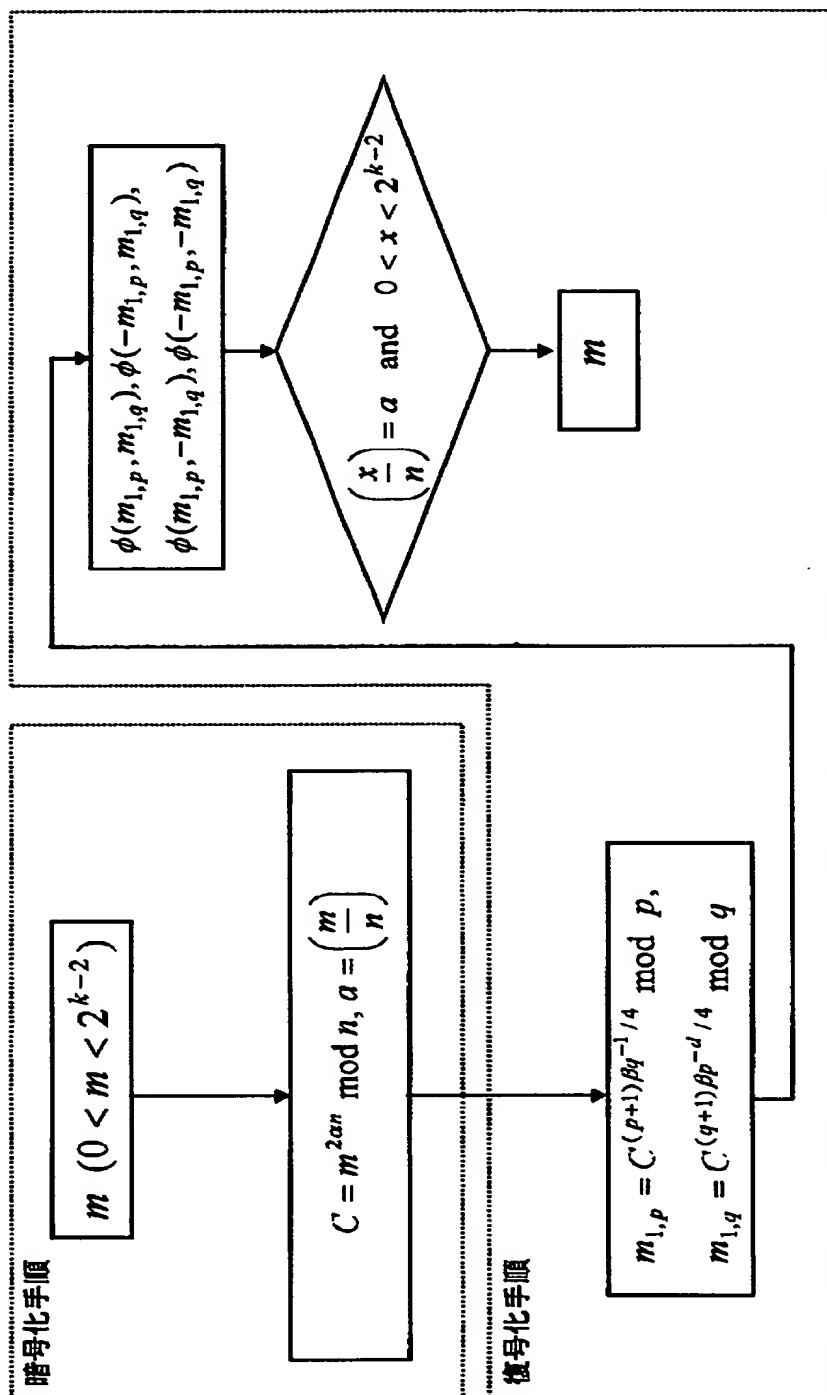
図 3



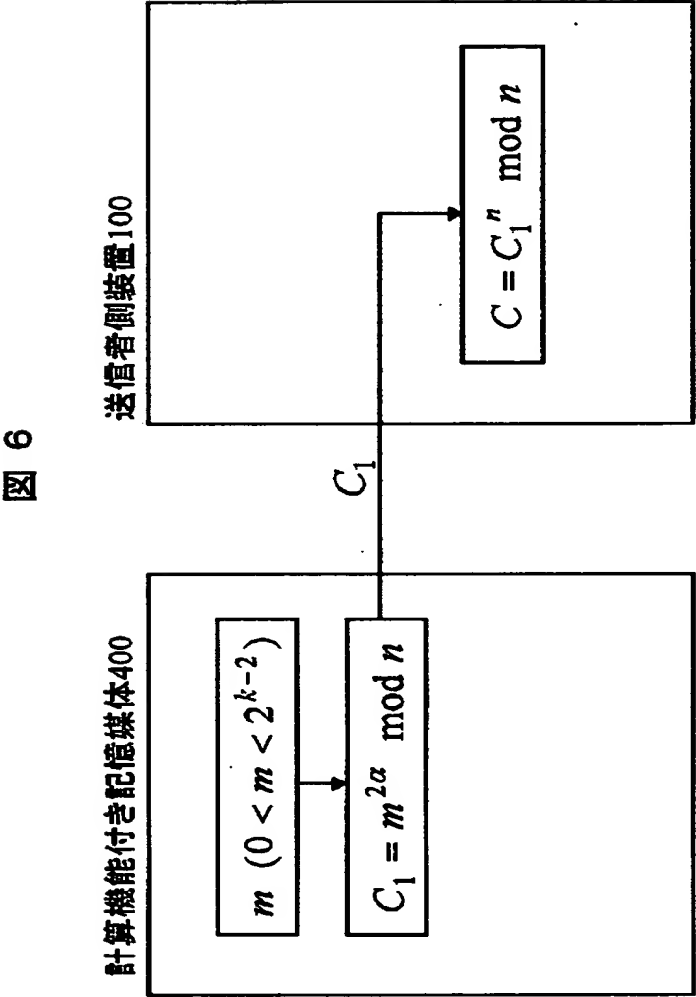
【図 4】



【図 5】

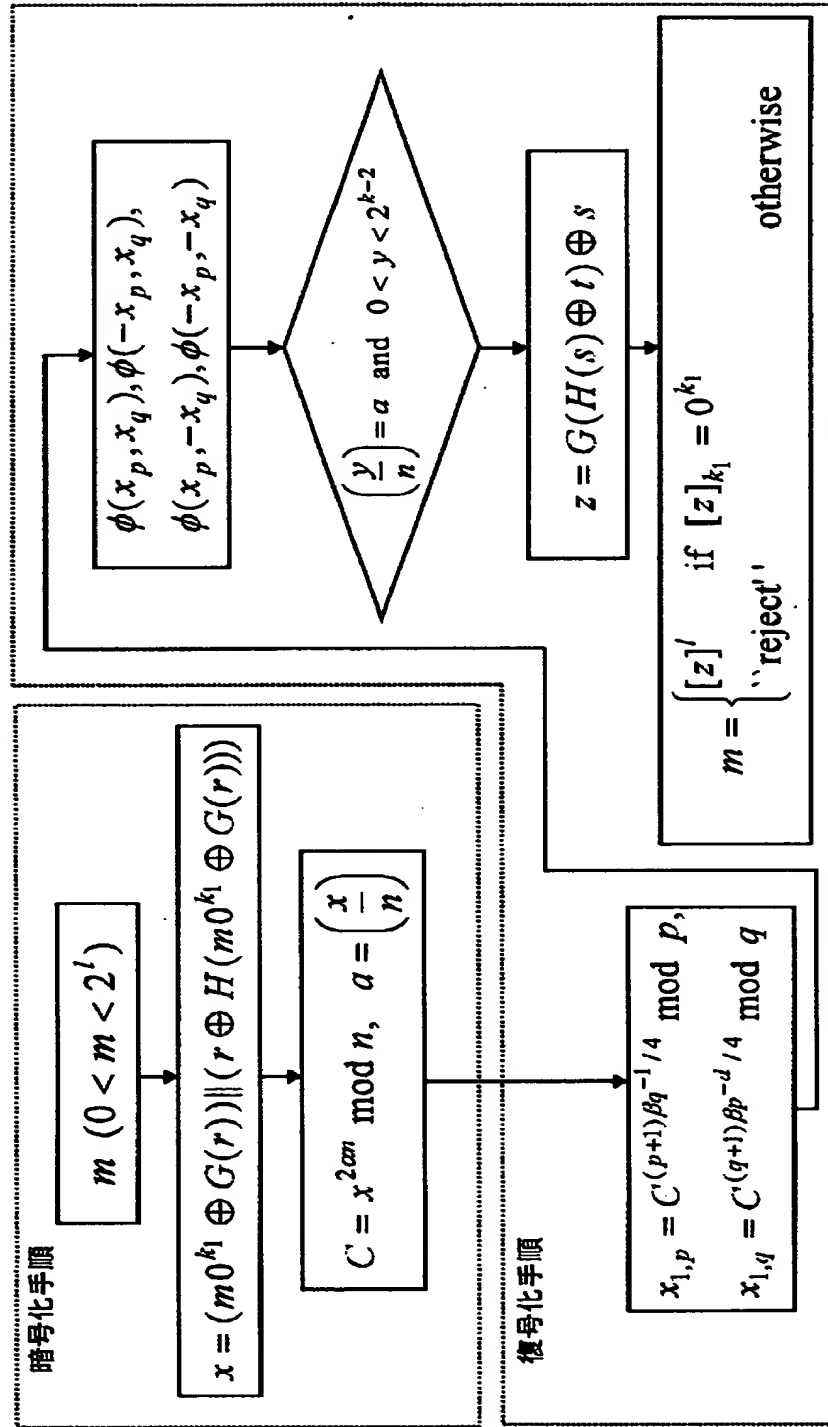


【図 6】



【図7】

図 7



【図 8】

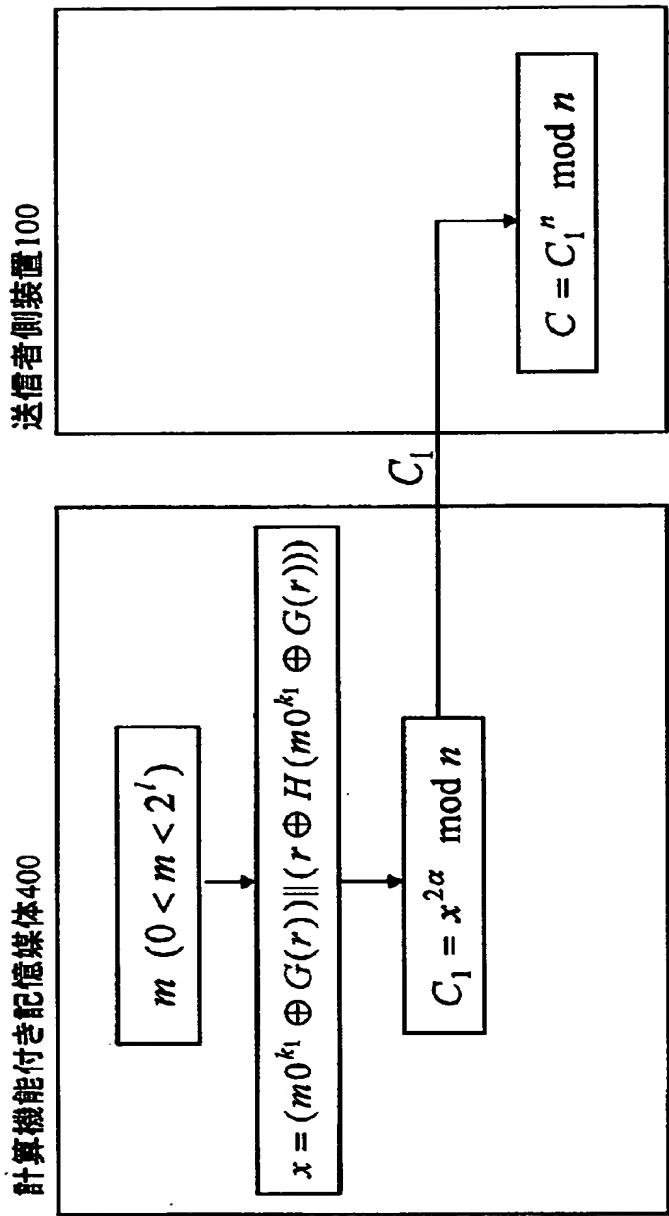
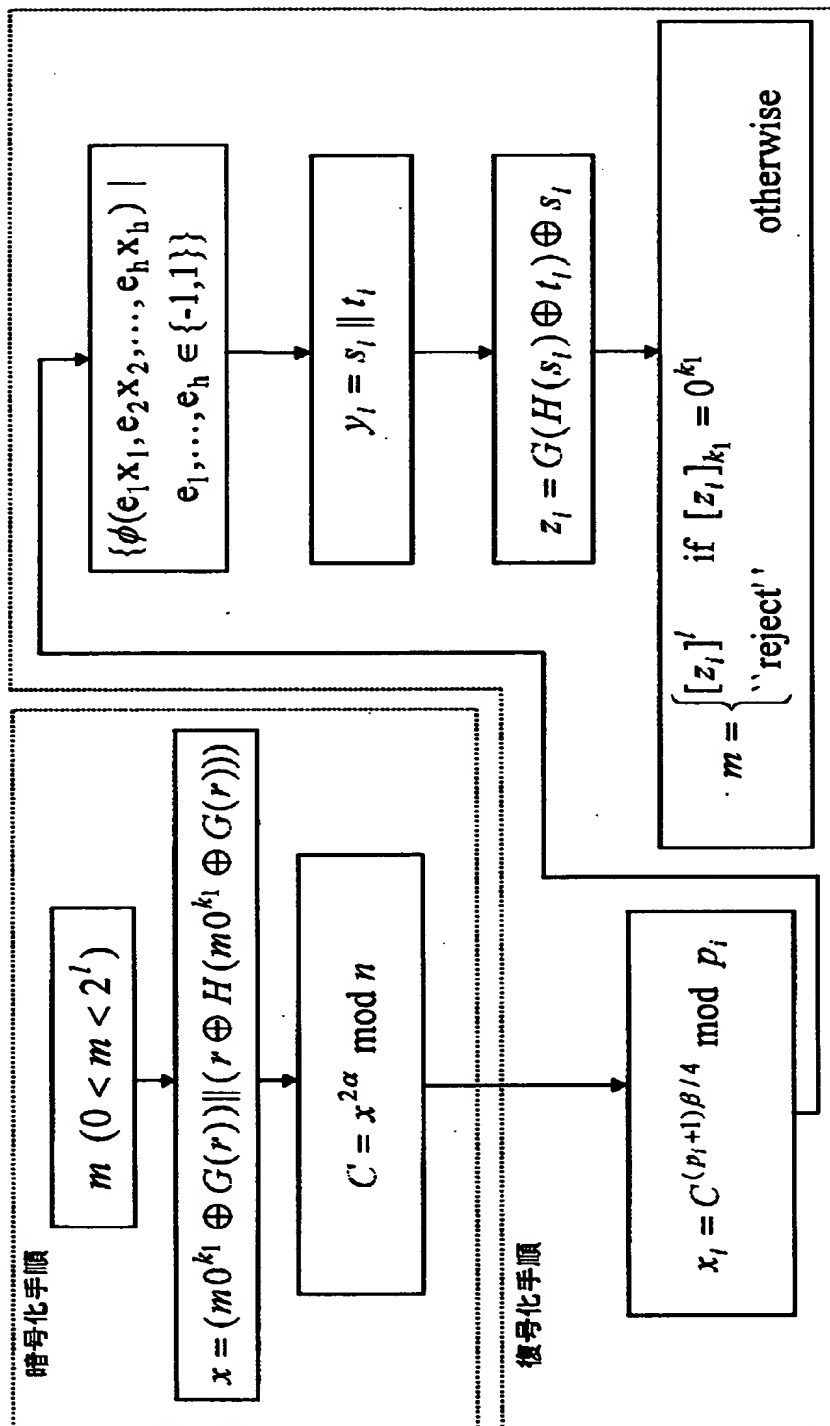


図 8

【図 9】

図 9



【図 1 0】

図 10

	暗号化	復号化	IND-CCA2
RSA	約 2~1500	約 400	No
ElGamal暗号	約 3000	約 1500	No
楕円曲線暗号	約 120	約 60	No
OAEP	約 2~1500	約 400	Yes
実施例11の方式	1	約 110	Yes

【書類名】 要約書

【要約】

【課題】

送信者は受信者の公開鍵を用いて送信者側装置100内で暗号文を作成し、通信回線300を介して受信者側装置200に送信し、受信者は秘密鍵を用いて暗号文の復号化を行う公開鍵暗号による暗号通信方法であって、安全性の証明が可能であり、かつ、効率性の高い公開鍵暗号方法を提供する。

【解決手段】

$n=p^d q$ (p, q は素数, pq は k ビット) に対して、平文空間を開区間 $(0, 2^{k-2})$ と小さな剰余群の部分集合となるように設定し、かつ、複数次存在する2次方程式の解の関係を明確化できるようにアルゴリズムを構成する。これにより、素因数分解問題の困難性との等価性により安全性の証明が可能となり、かつ、従来方式に比べてより高速な復号化処理が可能となった。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所